REMARKS

Applicant requests the Examiner to contact the undersigned to schedule a telephone interview to be conducted before a next action in this application. This request was also made by e-mail on January 3, 2009.

Claim 5 has been amended to depend on claim 3 rather than canceled claim 4.

Claims 1, 3, and 5-10 have been examined, with all claims rejected based on prior art. Claims 1, 3, 5, 7, 9, and 10 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Niessen et al. (U.S. Patent No. 5,367,638; hereinafter "Niessen") in view of Dias (U.S. Patent No. 4,855,690). Claims 6 and 8 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Niessen and Dias in view of Read et al. (U.S. Patent No. 5,353,243; hereinafter "Read").

Applicant respectfully traverses the prior art rejections for the following reasons.

The present application is concerned with techniques of preventing unauthorized external access to the operation of integrated digital circuits. The subject application is particularly concerned with countermeasures against the so-called side-channel attacks which are performed by unauthorized parties for analyzing integrated circuits, for example, for analyzing coding algorithms performed by a cryptocoproccessor.

In accordance with a first aspect of the application, the external detection of operations in a digital integrated circuit comprising an asynchronous circuit is prevented by time-varying a supply voltage of the asynchronous circuit to time-shift the execution of operations within the asynchronous circuit, wherein the time-variation of the supply voltage takes place in a random way.

In accordance with a second aspect of the application, a digital integrated circuit comprises an asynchronous circuit and means for time-varying a supply voltage of the asynchronous circuit to time-shift the execution point of operations within the asynchronous circuit, wherein the means for time-varying the supply voltage comprises a random number generator.

The Examiner concedes on page 4, lines 2-3 of the final Office Action that Niessen does not disclose that time variation takes place in a random way. In an attempt to make up for this deficiency, the Examiner applies Dias. The Examiner asserts at page 2, last paragraph, fourth line, that "The 103 combination of Niessen and Dias proposes the inclusion of the random number generation feature of Dias and using the concept of this feature to control the timing of voltage within the already established features or limitations of the Niessen invention."

The Examiner continues by asserting that "Even with a random signal at the filling degree signal the filling should still occur." The Examiner asserts on page 3, first sentence, of the Office Action that in his opinion there is no indication that the desired filling degree control of Niessen would no longer work (when replacing the feedback-control of the filling degree of Niessen by the random number generation feature of Dias).

To establish a prima facie case of 35 U.S.C. 103 obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skilled in the art to modify the reference or combine the reference teachings (MPEP 2143.01). Second, there must be a reasonable expectation of success (MPEP 2143.02). Additionally, the teaching or suggestion to make the claimed combination and the reasonable expectation of success must be found in the prior art, not in applicant's disclosure (In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991)).

These requirements intended to prevent unacceptable combinations have not been met by the Examiner.

To be more specific, Niessen discloses a digital data processing circuit in an apparatus comprising a data source which feeds a buffer for intermediate storage of data and subsequent outputting thereof and comprising a feedback circuit which, under control of a filling degree signal of the buffer, dynamically controls the data handling rate of the data source (see column 1, lines 7-12).

The digital apparatus comprises a data source including an integrated digital data processing asynchronous electronic circuitry based on self-timed elements, wherein the operating speed of the electronic circuitry is directly determined by its power supply voltage (see column 8, lines 41-46).

The feedback means controls the source of power supply voltage to vary the actual supply voltage provided to the electronic circuitry so as to dynamically control the data handling rate of the data source as a function of a filling degree signal reflecting the filling degree of a buffer storage means (see column 8, lines 50-60).

When replacing in the circuitry of Niessen the feedback control means which is responsive to the filling degree signal by a random generator or by a signal varying the supply voltage in a random way, then the desired filling degree control of Niessen would no longer work. Thus, there cannot be any reasonable expectation of success for one of ordinary skill to modify the circuitry of Niessen as proposed by the Examiner. Moreover, neither Niessen nor Dias contain any teaching or suggestion that would motivate one skilled in the present field to replace the filling degree feedback control for the buffer storage means of Niessen by a random signal.

The Examiner's argument outlined in the penultimate sentence of page 2 of the final Office Action that even with a random signal as the filling degree signal the filling of the Niessen technique should still occur is technically incorrect. Clearly, the filling degree signal must reflect the filling degree of the buffer storage means (column 8, lines 50-60). If the filling degree signal varies in a random way rather than reflecting the filling degree of the buffer storage means, then the buffer storage means would either run empty or would be over-filled. Thus, one skilled in the present field would necessarily understand that any feedback control signal in the technique of Niessen which does not reflect the filling degree of the buffer storage means would render the technique of Niessen technically useless. A technically useless control which can neither prevent the running-empty of the buffer storage means nor prevent an overfilling thereof would not be taken into consideration as a reasonable replacement of Niessen's technique to make use of a feedback signal reflecting the filling degree of the buffer storage means.

Thus, the claims are patentable over the applied references for at least these reasons.

In view of the above, Applicant believes the pending application is in condition for allowance.

In the event a fee is required or if any additional fee during the prosecution of this application is not paid, the Patent Office is authorized to charge the underpayment to Deposit Account No. 50-2215.

Dated: January 5, 2009

Respectfully submitted,
/Laura C. Brutman/
By_____
Laura C. Brutman
Registration No.: 38,395
DICKSTEIN SHAPIRO LLP
1177 Avenue of the Americas
New York, New York 10036-2714
(212) 277-6500
Attorney for Applicant